Why SATS Needs Formal Verification

Victor Carreño

NASA Langley Research Center

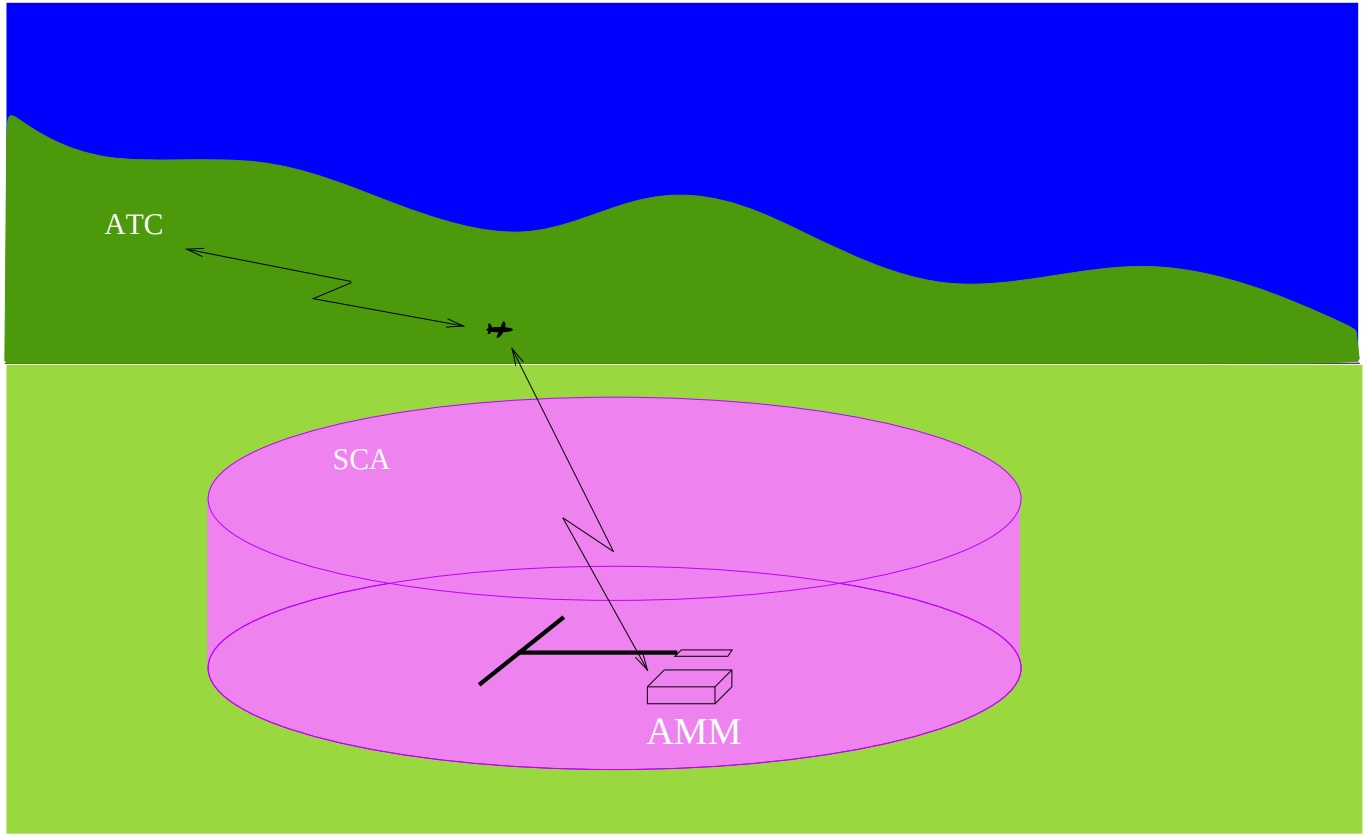
October 2003

SATS HVO Characteristics, I

SATS High Volume Operations (HVO) Concept of Operations is a Major departure from the state of practice.

In the USA and elsewhere in the world, IFR aircraft are positively controlled at all times by a human operator. Responsibility for separation is *always* in the hands of the controller.

SATS HVO Characteristics, II



SATS HVO Characteristics, III

- Use of automation to control traffic flow.
- No ground human operator.
- Pilot has separation responsibility in an IFR operation.
- Acceptability is based on its viability, safety, and reliability.
  - By regulatory agencies.
  - By flight crews.
  - By passengers.

Verification, I

- Assurance of intended functionality.
- Assurance of no undesirable behavior.
- There should be convincing evidence that the SATS HVO CONOPS is:
  - Safe
  - Correct
  - Feasible
- Methods of verification with a high degree of rigor will provide an intellectually justifiable argument.
- Development of the concept by thinking of "scenarios" is necessary but not sufficient.

Verification, II

- The combination of states and sequences of states is large and it is likely that some conditions will not be considered.

- A mathematical approach will allow for the exploration of all possible states and sequences.

Mathematical Verification is not Sufficient

- Like other engineering disciplines, simulation and testing are integral to the development process.
- Mathematical models need to be validated.
- Assumptions made in the mathematical analysis are validated by simulation.
- Assumptions made in simulations are validated in testing.

The State Explosion

- A system with three states, $\{a,b,c\}$, has 96 possible distinct sequences of length 6. (where state n is not the same as state n-1)
- A system with four states has 972 distinct sequences of length 6.
- A system with 1000 states has 9.9501 x 10^{17} distinct sequences of length 6.

Of course, in a physical system, only a fraction of the sequences are possible.

Nevertheless, it is nearly impossible for a person to mentally reason about all the interactions of a complex system.

Preliminary Discrete Model of SATS HVO CONOPS

- A preliminary discrete model has been created.
- This model has more than 2500 states.
- The number of possible sequences of states is very large.
- Construction of the model has lead to assumptions that should be added as part of the rules to the requirement specifications document.
- Checking of the model has revealed some sequences that are undesirable.
- Recommendations will be made to the SATS HVO CONOPS working team.
- The model will be refined and extended to make it more accurate and comprehensive.

Conclusion

- Formal Methods add value to the development process.
- Formal Methods is essential to a comprehensive verification process.
- Formal Methods will probably be beneficial to subsequent processes such as certification and social considerations.